Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

ChatGPT ff.:

→ Konsequenzen für die IT-Sicherheit

Prof. Dr. (TU NN)
Norbert Pohlmann
Vorstandsmitglied eco – IT-Sicherheit
***Professor** für **Cyber-Sicherheit** und*
Leiter** des **Instituts für Internet-Sicherheit – if(is)
Westfälische Hochschule, Gelsenkirchen

if(is) internet-sicherheit.

Thesen *(Blickwinkel Cyberkriminelle)*
→ Konsequenzen für die IT-Sicherheit

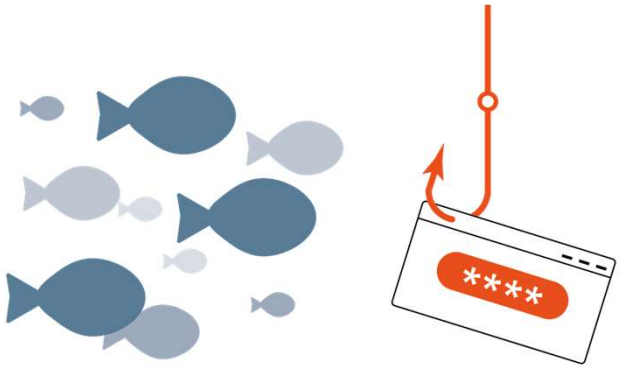
ChatGPT wird zunehmend dafür sorgen, dass Cyberkriminelle erfolgreicher angreifen können.

Nicht direkt, ***aber indirekt.***

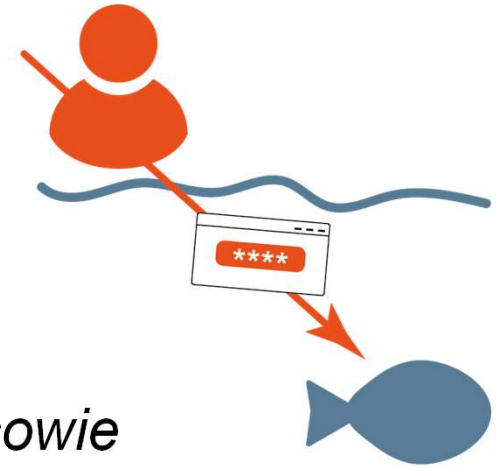
Cyberkriminelle ohne entsprechendes Know-how werden auch mit ChatGPT nicht plötzlich zu Profis.

Risiko
→ Phishing / Spear-Phishing

- Mit einem **Phishing-Angriff** versuchen Cyberkriminelle z. B. mithilfe von gefälschten Webseiten, **E-Mails** oder Kurznachrichten an **sensible Daten von Nutzern** zu gelangen und damit **Identitätsdiebstahl** zu begehen oder **IT-Systeme mit Malware zu infizieren**.



- Beim **Spear-Phishing** werden im Vergleich zum Phishing **individuelle Empfänger** sorgfältig **ausgewählt** und über sie **recherchiert**.
Die individuellen Opfer erhalten z. B. E-Mails, die auf sie persönlich zugeschnitten sind. Dadurch wirken diese viel glaubwürdiger und haben eine **höhere Erfolgswahrscheinlichkeit**.

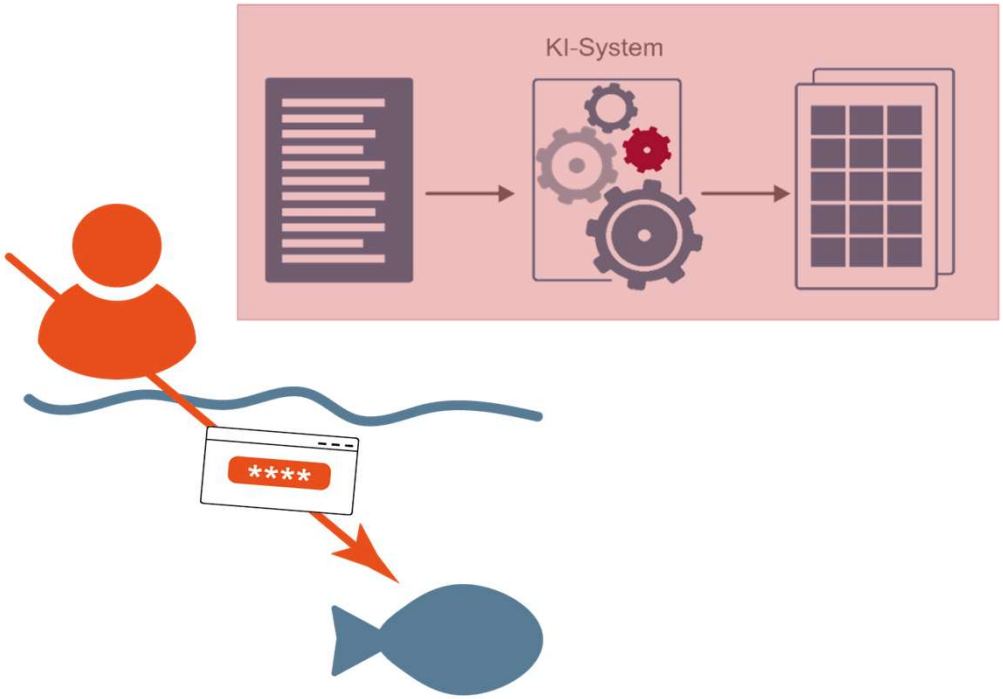


- *In Sozialen- und Berufsnetzwerken lassen sich Hobbys sowie Interessen identifizieren, um daraus **persönliche Spear-Phishing-Mails durch Cyberkriminelle zu formulieren**.*

Risiko

→ AI-Phishing / AI-Spear-Phishing

- Mit den neuen Sprachmodellen wie ChatGPT sind Cyberkriminelle in der Lage, *hochgradig individuelle* **AI-Spear-Phishing-Mails** zu generieren, die **deutlich wirksamer und gefährlicher** sind.
- *Mit der Einbindung von ChatGPT werden Spear-Phishing-Mails auf Basis der vielen verfügbaren personenbezogenen Daten **automatisiert** erstellt. Dadurch haben diese **AI-Spear-Phishing-Mails eine höhere Vertrauenswürdigkeit und Erfolgsaussichten**.*



Professionalisierung von Betrugspraktiken

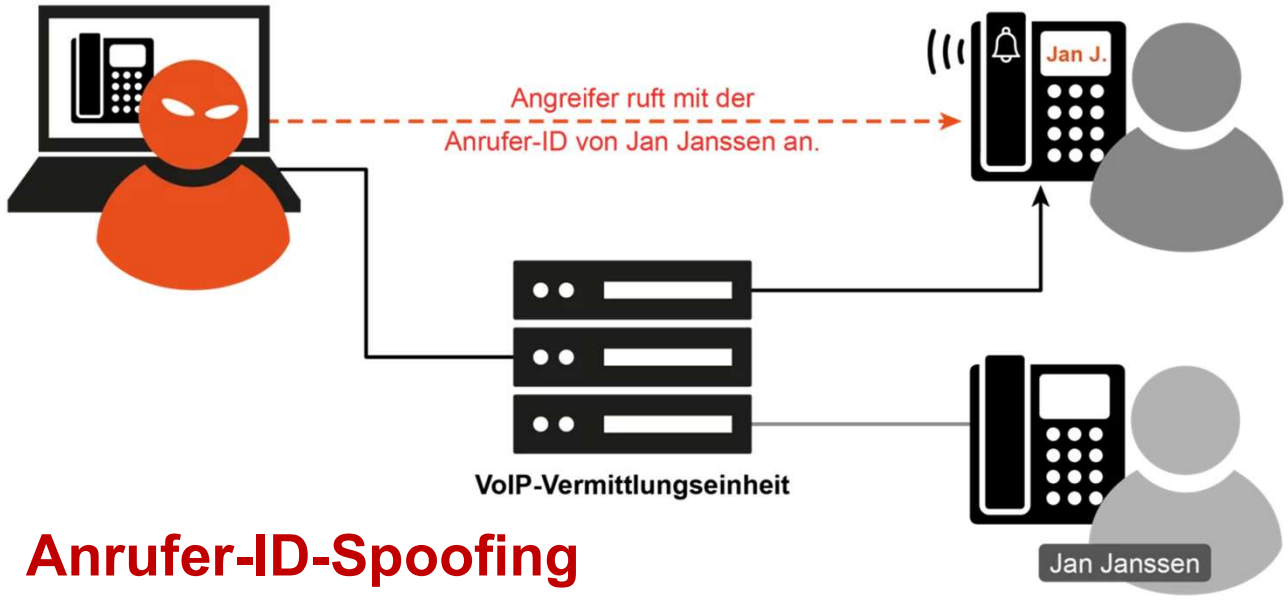
Gilt auch für Spam-Mails

Risiko
→ Fortschrittliches Social Engineering

- Die Tatsache, dass ChatGPT **menschenähnlich antwortet** macht Betrug mittels **Social Engineering** wesentlich **einfacher**.

- In Kombination mit *KI-generierten* **Bilder von Personen**, ***Audio-Imitationen*** und **Deepfake-Videos** stehen den Angreifern Techniken zur Verfügung, um moderne Social Engineering-Ansätze sehr gut und einfach umzusetzen.

- Ideal für **CEO-Angriffe**.



Anrufer-ID-Spoofing

Risiko
→ Beschleunigtes Entwickeln von Angriffen

- Bei der Erstellung von Malware und weiteren Angriffstechnologien kann **ChatGPT als wertvolles Hilfsmittel** genutzt werden.

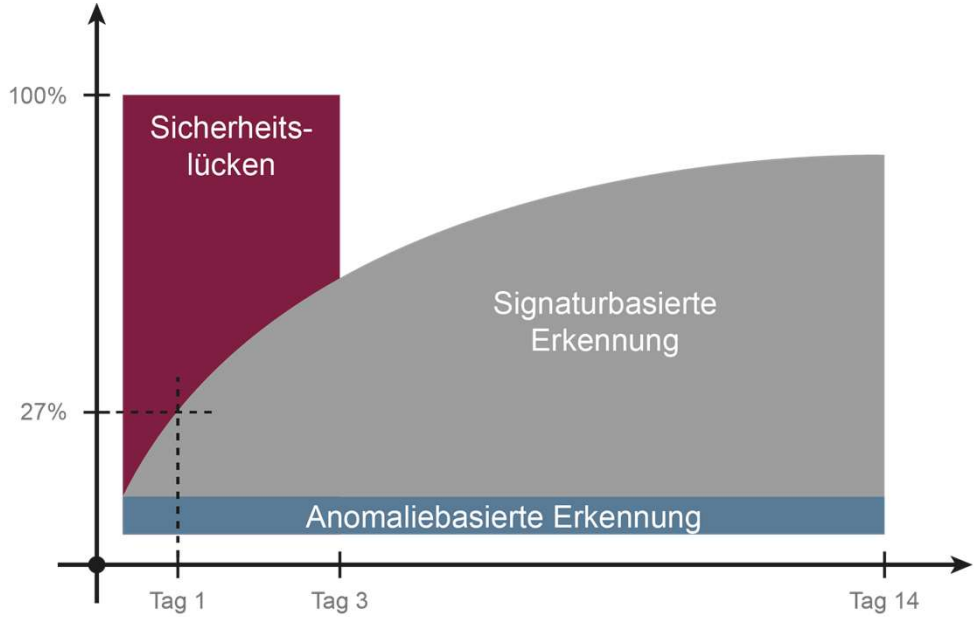
- Es ist zurzeit **nicht möglich**, dass **weniger erfahrene Angreifer ohne** jegliche Programmierkenntnisse **per Knopfdruck** funktionierende **Malware erstellen** können.

- Aber wenn ein **erfahrender Programmierer** ChatGPT als Assistent nutzt, ist er deutlich schneller als ohne. … ***weiße Blatt Syndrom*** …

Fachkräftemängel beseitigen

Risiko
→ Polymorphe Malware

- Bei ChatGPT kann durch **wiederholtes Fragen** die Antwort, also in diesem Fall der **Code variieren oder mutieren**.
- Dadurch kann mithilfe von ChatGPT einfach und automatisiert der Code geändert und **polymorphe Malware** umgesetzt werden.
- Somit wird die **Erkennungsrate** durch Schutzmechanismen **sinken**.
- *Aus diesen Gründen ist in Zukunft insgesamt mit mehr Malware- bzw. Ransomware-Vorfällen zu rechnen.*

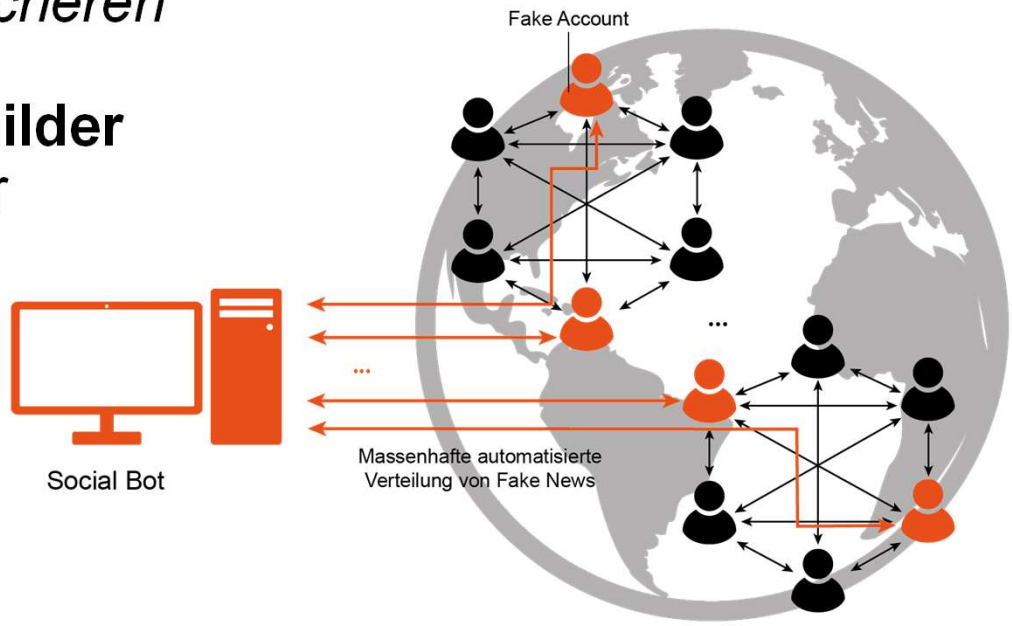


Risiko
→ Vertrauliche Informationen

- Die Inputs, die bei ChatGPT eingegebenen werden, beinhalten in vielen Fällen vertrauliche, sensible Informationen (Studie: **11 %** bei ChatGPT).
- Beispiele für die Nutzung von vertraulichen, sensiblen Informationen:
  - **Bankangestellte**, die Kundentermine vorbereiten (Vermögen, Anlagedetails …)
  - **Softwareentwickler**, die sensiblen Code bearbeiten
  - **Mitarbeiter**: Weitergabe von Firmengeheimnissen (Verkaufszahlen, Einkaufspreise, Gehälter, Patentinformationen …)
- **Daten**, die eingegeben werden,
  - sollen *im Prinzip* auch die **KI trainieren**, um diese zu verbessern. *(OpenAI macht das nach eigenen Angaben nicht. Prob.: Überprüfbarkeit)*
  - haben eine **neue, zusätzliche Angriffsfläche**. *(IT-Sicherheit und **Vertrauenswürdigkeit** des Anbieters/Supply Chain)*
- **Selbst OpenAI rät dazu, keine sensiblen Informationen zu teilen.**

Risiko
→ Verbreitung von Falschinformationen

- ChatGPT kann auch digitale Propaganda-Maschinen (Social Bots) unterstützen.
- Social Bots sind Meinungsrobotoren, die z. B. in sozialen Netzwerken gezielt **Meinungen** oder **Fake News** verteilen.
- Mit *überzeugenderen* und *authentischeren* Inhalten können die Botschaften erfolgreicher sein, um **Stimmungsbilder zu beeinflussen** und mehr Follower zu generieren.



- Beispiele:

  Manipulationen von Wahlen,

  Börsenkurse beeinflussen,

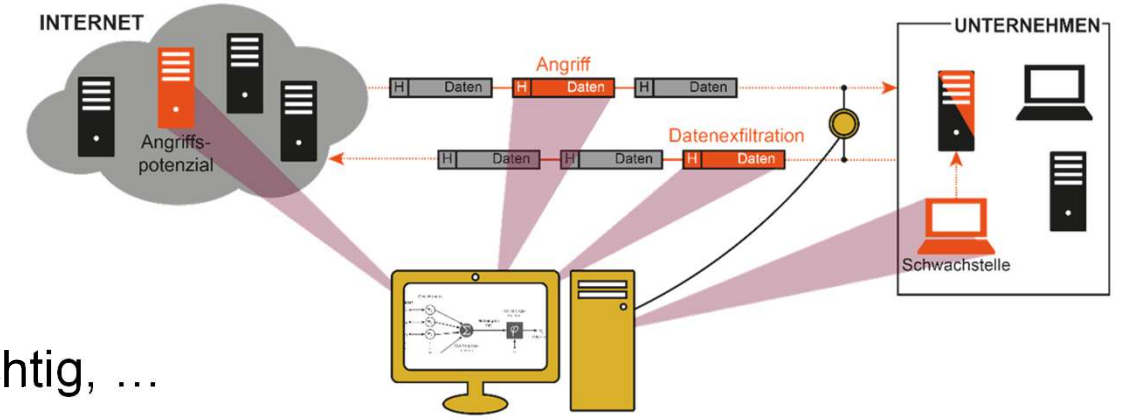
  politische Manipulationen

  (Geheimdienste oder Terrorgruppen)

  Cyber-Mobbing (Personen, Unternehmen und Produkte diskreditieren …)

  …

Cyber-Sicherheit *braucht*
→ Künstliche Intelligenz - Übersicht



- Erhöhung der **Erkennungsrate** von **Angriffen**
  - Netzwerk, IT-Endgeräte …
  - adaptive Modelle
  - Unterschied: normal und verdächtig, …

- **Unterstützung / Entlastung** von **Cyber-Sicherheitsexperten**
  - Erkennen von **wichtigen** sicherheitsrelevanten Ereignissen *(Priorisierung)*
  - **(Teil-)Autonomie** bei Reaktionen … Erhöhung der Resilienz …

- **Verbesserungen** von bestehenden **Cyber-Sicherheitslösungen** durch **KI**
  - zur Erhöhung der **Wirkung** und **Robustheit**, z.B.: Risiko-basierte und adaptive Authentifizierung
  - um **Schäden** zu **vermeiden** und **Risiken** zu **minimieren**!

Weitere Bereiche: Erkennung von Malware, Spam, Fake News, Deep Fake, usw.
sichere Softwareentwicklung, IT-Forensik, Threat Intelligence …

KI-Chatbots - Einfluss - IT-Sicherheit
→ Zukunftsaussichten

- **KI-Chatbots** werden in der Zukunft einen *signifikanten Einfluss* auf die **IT-Sicherheit** haben.
- Davon können sowohl **Angreifer** als auch **Verteidiger** profitieren.
- **KI-Chatbots** werden die **Cyber-Bedrohung** durch Cyberkriminelle erheblich **vergrößern** *(AI-Spear-Phishing, Social Engineering, polymorphe Malware, Analyse der / Angriffe auf Eingaben …)*
- **KI-Chatbots können auch die Cyber-Sicherheit verbessern.**
- Aufgrund der Fähigkeit, Eingaben in natürlicher Sprache zu verstehen und darauf reagieren zu können *(Detektion unerwünschter Inhalte, Mitarbeiterschulungen, Überwachung von Bedrohungen, Berichterstellung …).*
- **Zum Fixen von *Bugs* nutzen**, um die Sicherheit der Software zu erhöhen. *(Forschungsidee, mit einem sehr großen Einfluss auf die IT-Sicherheit.*
- **→ Fachkräftemangel bewältigen**

Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

ChatGPT ff.:

→ Konsequenzen für die IT-Sicherheit

Cyberkriminellen werden ChatGPT nutzen, die Verteidiger müssen dies auch tun.

Prof. Dr. (TU NN)

Norbert Pohlmann

Vorstandsmitglied eco – IT-Sicherheit

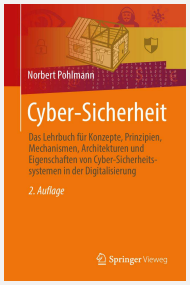
***Professor** für **Cyber-Sicherheit** und*
Leiter** des **Instituts für Internet-Sicherheit – if(is)
Westfälische Hochschule, Gelsenkirchen

Anhang / Credits

Wir empfehlen

Cyber-Sicherheit

Das **Lehrbuch** für Konzepte, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung“, Springer Vieweg Verlag, Wiesbaden 2022
https://norbert-pohlmann.com/cyber-sicherheit/



7. Sinn im Internet (Cyberschutzraum)

https://www.youtube.com/cyberschutzraum

CYBER SCHUTZRAUM

Master Internet-Sicherheit

https://it-sicherheit.de/master-studieren/

(M) MASTER internet-sicherheit.

Glossar Cyber-Sicherheit

https://norbert-pohlmann.com/category/glossar-cyber-sicherheit/

Cyber-Sicherheit GLOSSAR

It‘s all about Trust!

https://vertrauenswürdigkeit.com/

Besuchen und abonnieren Sie uns :-)

WWW
https://www.internet-sicherheit.de

Facebook
https://www.facebook.com/Internet.Sicherheit.ifis

Twitter
https://twitter.com/_ifis

https://twitter.com/ProfPohlmann

YouTube
https://www.youtube.com/user/InternetSicherheitDE/

Prof. Norbert Pohlmann
https://norbert-pohlmann.com/

Der Marktplatz IT-Sicherheit

(IT-Sicherheits-) Anbieter, Lösungen, Jobs, Veranstaltungen und Hilfestellungen (Ratgeber, IT-Sicherheitstipps, Glossar, u.v.m.) leicht & einfach finden.
https://www.it-sicherheit.de/

Quellen Bildmaterial

Eingebettete Piktogramme: Institut für Internet-Sicherheit – if(is)

Literatur

D. Adler, N. Demir, N. Pohlmann: „Angriffe auf die Künstliche Intelligenz – Bedrohungen und Schutzmaßnahmen“, IT-Sicherheit – Mittelstandsmagazin für Informationssicherheit und Datenschutz, DATAKONTEXT-Fachverlag, 1/2023
https://norbert-pohlmann.com/wp-content/uploads/2023/03/448-Angriffe-auf-die-Kuenstliche-Intelligenz-%E2%80%93-Bedrohungen-und-Schutzmassnahmen-Prof-Norbert-Pohlmann.pdf

U. Coester, N. Pohlmann: „Vertrauenswürdigkeit schafft Vertrauen - Vertrauen ist der Schlüssel zum Erfolg von IT- und IT-Sicherheitsunternehmen", DuD Datenschutz und Datensicherheit – Recht und Sicherheit in Informationsverarbeitung und Kommunikation, Vieweg Verlag, 2/2022
https://norbert-pohlmann.com/wp-content/uploads/2022/04/439-Vertrauenswuerdigkeit-schafft-Vertrauen-Prof-Norbert-Pohlmann.pdf

N. Pohlmann: „Wertschöpfung der Digitalisierung sichern - Vier Cybersicherheitsstrategien für den erfolgreichen Wandel in der IT“, IT-Sicherheit – Mittelstandsmagazin für Informationssicherheit und Datenschutz, DATAKONTEXT-Fachverlag, 1/2020
https://norbert-pohlmann.com/wp-content/uploads/2019/08/408-Wertsch%C3%B6pfung-der-Digitalisierung-sichern-Vier-Cybersicherheitsstrategien-f%C3%BCr-den-erfolgreichen-Wandel-in-der-IT-Prof.-Norbert-Pohlmann.pdf

N. Pohlmann: „Künstliche Intelligenz und Cybersicherheit - Unausgegoren aber notwendig“, IT-Sicherheit – Fachmagazin für Informationssicherheit und Compliance, DATAKONTEXT-Fachverlag, 1/2019
https://norbert-pohlmann.com/wp-content/uploads/2019/04/393-K%C3%BCnstliche-Intelligenz-und-Cybersicherheit-Unausgegoren-aber-notwendig-Prof.-Norbert-Pohlmann.pdf

N. Pohlmann: **Lehrbuch „Cyber-Sicherheit“,** Springer Vieweg Verlag, Wiesbaden 2022 Druckausgabe (ISBN 978-3-658-36242-3) und eBook (ISBN 978-3-658-36243-0).

Weitere Artikel siehe: https://norbert-pohlmann.com/artikel/

Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Institut für Internet-Sicherheit
→ Vorstellung und Übersicht

Prof. Dr. (TU NN)
Norbert Pohlmann
Vorstandsmitglied eco – IT-Sicherheit

***Professor** für **Cyber-Sicherheit** und*
Leiter** des **Instituts für Internet-Sicherheit – if(is)
Westfälische Hochschule, Gelsenkirchen

if(is) internet-sicherheit.

Institut für Internet-Sicherheit
→ Prof. Norbert Pohlmann

Berufliche Erfahrungen: Unternehmer im Bereich IT-Sicherheit

- Geschäftsführender Gesellschafter der **KryptoKom** GmbH *(1988-1999)*
- Vorstandsmitglied der **Utimaco Safeware** AG *(1999-2003)*

Hauptamtliche Tätigkeiten: seit 2003

- **Informatikprofessor** für Cyber-Sicherheit *und*
- Geschäftsführender **Direktor des Instituts für Internet-Sicherheit** – if(is) an der Westfälische Hochschule

Ehrenämter:

- Vorstandsvorsitzender des **Bundesverbands IT-Sicherheit** – TeleTrusT
- Vorstandsmitglied des eco – **Verband der Internetwirtschaft** e.V.
- Vorstandsmitglied **EuroCloud** Deutschland_eco e.V.
- Mitglied des wissenschaftlichen Beirates der **GDD**
- Mitglied im Lenkungskreis Initiative „**IT-Sicherheit in der Wirtschaft**“ des BMWi
- Mitglied der Advisory Group der European Union Agency for Cypersecurity – **ENISA**
- …

Institut für Internet-Sicherheit
→ Übersicht

- Das Institut für Internet-Sicherheit - if(is) ist eine Fachbereich übergreifende, **wissenschaftliche Einrichtung der Westfälischen Hochschule,** im Fachbereich Informatik
- Gründung: 2005
- Wir haben uns zu dem **führenden Institut für Internet-Sicherheit** entwickelt!
- Seit WS10/11: **Master** „Internet-Sicherheit“
- Ca. 50 Mitarbeiter

- Unser **Ziel** ist es, einen Mehrwert an **Vertrauenswürdigkeit** und **Sicherheit** im Internet herzustellen.

Zahlen des if(is)

→ Übersicht

600+ Hacking-Shows
mit 12 unterschiedlichen Hackern

100 Forschungspartner
Firmen/Behörden 65 und Hochschulen 35

300+ Artikel / 400+ Vorträge / 30+ Bücher
national und international

150+ Fernsehauftritte
Tagesschau/-themen, WDR, ZDF, SAT1, 3SAT …

200+ Abschlussarbeiten
Diplom, Bachelor, Master und Promotionen

200+ wissenschaftliche *und* studentische **Mitarbeiter** (zurzeit sind es mehr ca. 40)

60+ Drittmittelprojekte
mit Unternehmen / Behörden

150+ Zeitungsinterviews
ZEIT, Focus, FAZ, Süddeutsche Zeitung, Handelsblatt, Welt, DPA …

54 Forschungsprojekte
BMBF 20, BMWK 10, BMDV 1, EU 4, NRW 15, BMI 4 …

4 Start-ups aus dem if(is)
finally safe; XignSys, TrustCerts, aware7

Forschungsschwerpunkte im if(is) internet-sicherheit.

- Internet Frühwarnsysteme
- (Internet-)Kennzahlen-Sys.
- KI + Cyber-Sicherheit
- Zahlungssysteme und Banktransaktionen
- Blockchain
- Identity Management
- IoT Security
- Gesundheitswesen
- Vertrauenswürdige IT-Systeme
- Smart City, -Car, -Traffic
- Cloud, Fog, Edge Computing
- Mobile Security
- Botnetz-Erkennung
- Vertrauenswürdigkeit